REMARKS

Applicants respectfully request that the subject application be preliminarily amended as provided in the foregoing amendment prior to calculation of the filing fees. Applicants also respectfully request the Examiner to consider the foregoing amended claims, the remarks provided in Applicants' Response to Final Office Action dated November 27, 2007, as well as the following remarks in the first Office Action on the merits.

Claim 1 was amended for clarity, to include a limitation of claim 2, and to more distinctly claim the present invention.

Claims 2 and 8 were amended to be consistent with the language of amended claim 1.

Claim 7 was canceled in view of the amendment to claim 1 and the dependency of each of claims 9 and 12 was amended to reflect the cancellation of claim 7.

Claims 17 and 18 were amended for clarity and to more distinctly claim the present invention.

Claim 21 was amended to be consistent with the language of amended claim 18.

The amendments to the claims are supported by the originally filed disclosure and thus entry of the foregoing amendments into the subject application is respectfully requested.

The amendments to the claims are supported by the originally filed disclosure and thus entry of the foregoing amendments into the subject application is respectfully requested.

35 U.S.C. §103 REJECTIONS

Claims 1-22 stand rejected under 35 U.S.C. §103 as being unpatentable over the cited prior art for the reasons provided on pages 3-10 of the Final Office Action mailed September 27, 2007. Because claims were amended in the foregoing amendment, the following discussion refers to the language of the amended claim(s). As claim 7 was canceled in the foregoing

amendment, Applicants, have not separately addressed this claim herein. However, only those amended features specifically relied on in the following discussion shall be considered as being made to overcome the prior art reference. The following addresses the specific rejections provided in the above-referenced Office Action.

CLAIMS 1-14, 17-22

Claims 1-14 and 17-22 stand rejected as being unpatentable over Burns et al. [USP 6,405,315; "Burns"] in view of Miyazaki et al. [US Patent Application Publication 2002/0174369; "Miyazaki"] for the reasons provided on pages 3-9 of the above-identified Final Office Action. As indicated above, claim 7 was canceled and thus, is not being addressed further herein. Applicants respectfully traverse.

As grounds for the rejection, the above-referenced Office Action provides that Burns et al describes a setting section for setting a security level for the data to be transmitted and that this security level is set by a user from a plurality of identified security levels, with reference to col. 9 lines 1-25 thereof. Applicants respectfully disagree.

Before discussing the details of the rejection, it appears that there may be some confusion as to a user of a network computer and the term "network client" in Burns. In its broadest meaning a network client is any resource that is connected to a network, this includes a computer, a printer, a communication link, or a software application. At no time does the term network client mean the user of a computer. In some cases, the software being executed or run on a computer also can be referred to as network client software. While a user can provide inputs or instructions to a computer, the inputs or instructions are carried out by the computer operating systems and applications programs and any instructions or criteria embedded in these programs. Thus, Applicants submit that Burns does not describe, teach or suggest the claimed invention to the extent that the rejections are based on the incorrect assumption that a network client simply equates to a user.

The discussion in Burns that includes the excerpt referred to in the grounds of the rejection reads as follows (See col. 8 line 65-col. 9 line 25).

LOCK MANAGER

> Locking and cache consistency will be handled by a distributed lock manager 34. The lock manager 34 handles the consistency of files on the level of network objects. Before a network client can change a network object, it must request a write lock from the lock manager. (Note: the network object itself doesn't handle any locking). Each lock requested has a lease associated with it. The lock becomes invalid when the lease expires, the client explicitly releases it, or the lock manager contacts the client to revoke the lock. When a client is contacted to revoke a lock, it must flush any pending changes for the locked region and then release the lock. When a client requests a read lock, the lock manager revokes any write locks held on the region before granting the read lock. When a client requests a write lock, the lock manager revokes any read and write locks held on the region before granting the lock. Note, for a file that is being read and written by multiple clients this method of locking will yield poor performance; however, studies have show that this access pattern occurs rarely in distributed file systems.

As can be seen from the foregoing, the language forming the basis for the rejection, does not in fact relate to the setting of a security level but rather this discussion relates to the process that is well known to those in the computer programming arts, involved with locking out access to an object during a write to ensure consistency of the object. This generally becomes a concern when the object is one which can be accessed by multiple network clients. In other words, one network client cannot update or revise a network object without the lock manager first locking the object out to access by others. As is well known to those in the computer arts, the write operation is initiated in the normal course by a user, but thereafter the actual writing operation to the storage device is carried out by the operating system and/or application systems.

As described above, the object is held in the locked out condition until the lock is revoked by the locking manager or released by the network client. As also described above, there is a similar locking function carried out when any network client is attempting to read the object. As

is indicated above, before a read is carried out, an existing lock must be revoked before the object can be read.

The assertion in the Office Action that the file system in Burns embodies a setting section also is not supported by other discussion therein. As can be seen from the Abstract (provided below) that the storage device in Burns serves as the repository of the system's data. The network client may have read or write access to a file being stored on storage device. Access is controlled using keys and access lists maintained by the key manager.

ABSTRACT

> A decentralized file system based on a network of remotely encrypted storage devices is disclosed. The file system includes a network to which a network client, a secure remotely encrypted storage device, a key manager, and a lock manager are attached. The system organizes data as files and directories. Files or directories are composed of one or more streams, which logically partition the data associated with the files or directories. *The device serves as a repository of the system's data.* The key manager controls data access keys while the lock manager handles consistency of the files. *A network user may have read or write access to a file. Access is controlled using keys and access lists maintained by the key manager.* (Italics added for emphasis)

As previously indicated by Applicants, as described in Burns (see col. 5, lines 25-35 excerpted below), data is remotely encrypted by the network clients (the components of the file system that request data from the storage devices), travels over the network in encrypted form and is stored in encrypted form on the storage device(s). This language also suggests that the term "network client" is referring to the software being executed on a computer. It should be noted that nowhere in this discussion is it provided that the user selects a security level as it is clear from the below discussion that all objects are being encrypted before transmission, which hardly bespeaks of a use selecting a security level.

> To support the decentralized remotely encrypted file system of the present invention, the storage devices are used as repositories of the file system's encrypted data and metadata. *Data is remotely encrypted by the network clients (the components of the file system that request data from the devices), travels*

> *over the network in encrypted form, and is stored encrypted on the devices.* The advantage of this approach is that data is encrypted or decrypted by the clients as opposed to having the encryption being done at both the devices and the clients. *Each network storage device is an independent entity on which the unit of storage is a network object.* The devices authorize network access to the network objects using MACs (Message Authentication Code). See, for example, "HMAC: Keyed-hashing for Message Authentication," Krawczyk et al., Request For Comments 2104, February 1997. *When a network client wants to update file system data, it reads the network object to be changed, decrypts the data, performs the change, and re-encrypts the data. It then sends a request to the network storage device to replace the old data, and authenticates the request with a MAC done using the change key corresponding to the object.* (Italics added for emphasis)

As also previously indicated by Applicants Burns (see col. 5, lines 47-55 thereof) further describes that the network storage device is trusted to store the encrypted file system data (not sent back old or garbage data) but the network storage device is not trusted to keep the data secret. Instead each such device has a device owner that controls access to the device data by setting up for example, subscribers with authority to create objects on the device (see Burns col. 5, lines 56-65).

In sum, Burns does not describe, disclose or suggest anywhere a setting section for setting a security level for the data to be transmitted, the set security level being selected by a user from a plurality of identified security levels. This is not surprising as Burns effectively describes storing data at one security level.

Applicants respectively disagree with the assertion that that Miyazaki describes setting data to be transmitted at one of a plurality of security levels and that it would have been obvious to modify Burns in view of the teachings of Miyazaki.

Miyazaki does teach that there can be more than one security level, and Miyazaki also teaches that a user could specific a security level when creating a document or file. Miyazaki, however, does teach that additional restraints are imposed in connection with the reading and writing process. Specifically, Miyazaki teaches that a user can access and save data in or create a

new file that has a security designation that is at his designated security level or higher, however, the user cannot save a file at a lower security level. Miyazaki also teaches that a user can only read a file that is at or lower than hid security level. Thus, for example, a person having the highest security level in the system could create a file and update the data in such a file only whose classification is at the highest security level. In sum, the ability to write in more than one security level, is a matter of what security level a user has and the practicality of a user with that security level creating a file that would be in a higher security classification.

In addition, Miyazaki is directed to a centralized computer system or host computer system in which information is stored in a centralized location and functions. This host computer is a server that has two operating systems running on the computer, where one operating system, a host OS, accesses one memory and hard driver and the other operating systems, a guest OS, accesses another memory and hard drive. Miyazaki teaches that the guest operating system is provided to control the ability of users to access the information or files on the hard drive that is managed by the host OS. Basically, the guest OS imposes the above described limitations on access so that a user cannot read documents above their security level and cannot save a file at a security level that is below their security level.

Notwithstanding this and in the interests of advancing prosecution, Applicants amended claim 1 for clarity and to more distinctly claim the present invention. More specifically, Applicants amended the setting section clause of claim 1 to read as follows: a setting section for setting a security level for the data to be transmitted, wherein the setting section sets the security level responsive to an input from a user of the electronic device, where the set security level being selected by the user is selected from a plurality of identified security levels. It also is respectfully submitted that Burns nowhere describes the above as well.

The electronic device network system of claim 1 also includes a search means for searching the plurality of storing means and for searching the plurality of external devices to identify one of a given storing means or given external device whose security level corresponds

to the security level set in the setting section.

As indicated above, in Burns all of the information being transmitted is being encrypted and is being stored in the encrypted condition. Also, the storage devices in Burns are not trusted as that term is used in a security sense. Thus, it would be inherently inconsistent with the description and teachings in Burns to assert that the described file system would embody a search means for searching out storage means or devices having different security levels because quite simply there is none in Burns.

In Miyazaki, there is only one storage device on which information is being stored and which is accessible to a user, given that this system is a centralized storage system. Thus, it would be inherently inconsistent with the description and teachings in Miyazaki to assert that the described file system would embody a search means for searching out storage means or devices having different security levels because quite simply there is none in Miyazaki.

In sum, Burns alone or in combination with Miyazaki does not describe or teach a search means for searching the plurality of storing means and for searching the plurality of external devices to identify one of a given storing means or given external device whose security level corresponds to the security level set in the setting section as s set forth in claim 1.

Notwithstanding the foregoing and in the interests of advancing prosecution, Applicants amended claim 1 to further provide that the electronic device transmits the data to one of the given storage means or the given external device whose security level corresponds to the security level set in the setting section responsive to a selection by the user of the means or device as being the intended recipient of the data. This, aspect is not described anywhere in Burns or Miyazaki.

As to claims 2-3, 6 and 8-13, each of these claims depends (directly or ultimately) from claim 1. Thus, each of claims 2-3, 6 and 8-13 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 2-3, 6 and 8-13 are not separately patentable from the combination of

Burns and Miyazaki.

As to claim 17, Applicants respectfully submit that the above remarks regarding claim 1, apply to distinguish the data receiver search system of claim 17 from the combination of Burns and Miyazaki. This shall not, however, be considered an admission that there are not additional grounds for distinguishing claim 17 from the combination of Burns and Miyazaki.

As to claim 18, Applicants respectfully submit that the above remarks regarding claim 1 apply to distinguish the data receiver search method of claim 18 from the combination of Burns and Miyazaki. This shall not, however, be considered an admission that there are not additional grounds for distinguishing claim 18 from the combination of Burns and Miyazaki.

As to claims 19-22, each of these claims depends (directly or ultimately) from claim 18. Thus, each of claims 19-22 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 19-22 are not separately patentable from the combination of Burns and Miyazaki.

It is respectfully submitted that claims 1-6, 8-14 and 17-22 are patentable over the cited reference(s) for the foregoing reasons.

CLAIMS 15-16

Claims 15 and 16 stand rejected as being unpatentable over Burns et al. [USP 6,405,315; "Burns"] in view of Miyazaki et al. [US Patent Application Publication 2002/0174369; "Miyazaki"] and further in view of Tomat [USP 6,459,499]. Applicants respectfully traverse as discussed below. Because claims were amended in the instant amendment, the following discussion refers to the language of the amended claims. However, only those amended features specifically relied upon to distinguish the claimed invention from the cited prior art shall be considered as being made to overcome the cited reference.

Each of claims 15-16 depends (directly or ultimately) from claim 1. Thus, each of claims 15 and 16 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 15-16 are not separately patentable from the combination of Burns, Miyazaki and Tomat.

It is respectfully submitted that claims 15 and 16 are patentable over the cited reference(s) for the foregoing reasons.

The following additional remarks shall apply to each of the above.

As provided in the MPEPs, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *In re Jones*, 958 F. 2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). As provided above, the references cited, alone or in combination, include no such teaching, suggestion or motivation.

Furthermore, a prior art reference can be combined or modified to reject claims as obvious as long as there is a reasonable expectation of success. *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 19866). Additionally, it also has been held that if the proposed modification or combination would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. Further, and as provided in MPEP-2143, the teaching or suggestion to make the claimed combination and the reasonable suggestion of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). As can be seen from the forgoing discussion regarding the disclosures of the cited references, there is no reasonable expectation of success provided in the references that the suggested modification would be reasonably successful. Also, it is clear from the foregoing discussion that the modification suggested by the Examiner would change the principle of

operation of the system and methodology described in Burns.

It is respectfully submitted that for the foregoing reasons, claims 1-6 and 7-22 are patentable over the cited reference(s) and thus, satisfy the requirements of 35 U.S.C. §103. Therefore, these claims, including the claims dependent therefrom are allowable.

It is respectfully submitted that the subject application is in a condition for allowance. Early and favorable action is requested.

Applicants believe that additional fees are not required for consideration of the within Preliminary Amendment. However, if for any reason a fee is required, a fee paid is inadequate or credit is owed for any excess fee paid, you are hereby authorized and requested to charge Deposit Account No. **04-1105**.

Respectfully submitted,
Edwards Angell Palmer & Dodge, LLP

Date: February 22, 2008

By: **/ William J. Daley, Jr. /**

William J. Daley, Jr.
(Reg. No. 35,487)
P.O. Box 55874
Boston, MA 02205
(617) 239-0100

Customer No. 21,874

Bos2_659513